IN THE CLAIMS

Claim 1 has been amended as follows:

1. (Currently Amended) A method for protecting a security module comprising the steps of:

storing security relevant data in a non-volatile memory of a security module and inserting said security module in a device motherboard;

monitoring proper insertion of said security module on said device motherboard with a first function unit and a second function unit in said security module;

signaling at least one security-related status of said security module with said first function unit;

in said monitoring of proper insertion, detecting a status indicating at least one of improper use and improper replacement of said security module with said second function unit and, upon a detection of said status indicating at least one of said improper use and said improper replacement, said second function unit causing said security-relevant data to be erased;

in said monitoring of proper insertion, monitoring a continued existence of said status with said second function unit and detecting, with said second function unit, when said status no longer exists;

~~following at least one of proper use and proper replacement of said security module~~ when said second function unit detects that said status no longer exists, initiating re-initializing, with said first function unit, any erased, security-relevant data; and

after said re-initializing, enabling each of said first function unit and said second function unit to re-commission said security module.

Claim 2 (Cancelled).

Claim 3 has been amended as follows:

3. (Currently Amended) A method as claimed in claim 1 comprising the additional steps of:

storing security relevant data in a security module and inserting said security module in a device motherboard;

normally operating said security module with system voltage from a device containing said device motherboard and, in an absence of said system voltage, operating said security module with a batter; and

monitoring a status of said battery with said second function unit as ~~a basis for detecting~~ said status indicating at least one of said improper use and said improper replacement.

4. (Original) A method as claimed in claim 1 comprising providing a third function unit and inhibiting said security module with said third function unit during at least one of replacement of said security module on said device motherboard and damage to said security module.

5. (Original) A method as claimed in claim 4 comprising detecting said damage to said security module with said third function unit.

6. (Original) A method as claimed in claim 1 comprising evaluating a running time credit with said first function unit and, upon expiration of said time credit, signaling a suspicious status of said security module with said first function unit.

7. (Original) A method as claimed in claim 6 comprising the additional steps of:

after expiration of said time credit, said first function unit establishing a communication with a remote data source; and

restoring normal operation to said security module via said communication.

8. (Original) A method as claimed in claim 6 comprising selecting a duration of said time credit to obtain a time credit of selected duration, and loading said time credit of selected duration into a memory in said security module, said memory being accessible by said first function unit.

9. (Original) A method as claimed in claim 6 wherein said time credit is a first time credit, and comprising the additional steps of monitoring a second time credit with said first function unit, which is longer than said first time credit, and signaling a status designating a device containing said device motherboard as being inoperable when said second time credit expires.

Claims 10-16 (Cancelled).